

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Raymond E. Ozzie et al.
Serial No.: 10/631,206
Confirmation No.: 3320
Filed: July 31, 2003
For: METHOD AND APPARATUS FOR MANAGING AND DISPLAYING
CONTACT AUTHENTICATION IN A PEER-TO-PEER
COLLABORATION SYSTEM
Examiner: S. Zia
Art Unit: 2431

Certificate of Electronic Filing Under 37 CFR 1.8

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: September 30, 2009

Signature: 

INTERVIEW SUMMARY

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants thank the Examiner for the courtesy of initiating and conducting a telephone interview, which occurred during telephone calls on August 16 and August 24, 2009. In response to the Amendment after final filed September 7, 2009, the Examiner called to explain that Applicants had misunderstood the indication of allowable subject matter in the Final Rejection. The Examiner suggested changes substantially in the form attached.

Dated: September 30, 2009

Respectfully submitted,

By 

Edmund J. Walsh
Registration No.: 32,950
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
617.646.8000

PROPOSED CLAIM AMENDMENTS**August 24, 2009**

1. (Canceled)
2. (Previously Presented) The method of claim 43 wherein determining whether the display name of the second user is equivalent to the display name of the contact stored in the contact data store comprises computing a clean name from each display name and comparing clean names of the two display names.
3. (Canceled)
4. (Previously Presented) The method of claim 43 wherein generating a warning comprises displaying a name conflict indicator next to each display name associated with a contact identity whose authentication level (1) is less than the highest authentication/certification level of all contact identities with equivalent display names or (2) equals the highest authentication/certification level of all contact identities with an equivalent display name and at least one other contact identity with an equivalent display name has been identified having an equal authentication level.
- 5.-8. (Canceled)
9. (Previously Presented) The method of claim 43 further comprising:
preventing a user from communicating with another user based on a security policy when the other user has a predetermined authentication level.
10. (Currently amended) The method of claim 43 wherein generating the warning comprises displaying a dialog box having all display names that are equivalent to the display name of the first second user listed therein.

11. (Currently amended) The method of claim [[49]] 43 wherein the step of receiving user input comprises assigning the alternative display name as an alias to the selected display name which alias is not equivalent to either of the ~~first conflicted~~ display name and the selected display name and which alias replaces the selected display name.

12. (Previously Presented) The method of claim 43 wherein displaying the warning comprises: displaying an authentication indicator next to a display name that is not equivalent to another display name, which authentication indicator displays the authentication level of the associated contact.

13. (Original) The method of claim 12 wherein each contact can have one of a predetermined number of authentication levels and wherein the authentication indicator that is displayed is unique to one of the authentication levels.

14. (Canceled)

15. (Previously presented) The method of claim 51 wherein receiving an input setting a security policy comprises receiving from a user of the computing device the input setting the security policy.

16. (Previously presented) The method of claim 51 wherein receiving an input setting a security policy comprises receiving from a system administrator the input setting the security policy.

17. (Previously Presented) The method of claim 51 wherein selectively responding to the event comprises warning a user when the security policy is set to warn and the user attempts to communicate with an unauthenticated and uncertified contact.

18. (Previously Presented) The method of claim 51 wherein selectively responding to the event comprises preventing a user from communicating with an uncertified contact when the security policy is set to restrict and the user attempts to communicate with an uncertified contact.

19. (Previously Presented) The method of claim 51 wherein selectively responding to the event comprises allowing a user to communicate with an unauthenticated and uncertified contact when the security policy is set to allow without warning and the user attempts to communicate with an unauthenticated and uncertified contact.

20. (Previously Presented) The method of claim 51 wherein determining the authentication level of the first user comprises:

- compiling a contact list of contacts;
- checking the contact list to determine contacts that are not authenticated;
- checking the unauthenticated contacts to determine whether a certification policy applies to any unauthenticated contact; and
- placing an unauthenticated contact on the list of unauthenticated and uncertified contacts when no certification policy applies to that contact.

21-42. (Canceled)

43. (Currently amended) A method of operating a computing device providing an endpoint in a peer-to-peer collaboration system in which each user has an identity and a display name, the method comprising:

- in response to communicating with a first user, recording the first user as a contact in a contact data store in memory associated with the computing device, the recording comprising storing at least an identity and display name of the first user;
- in response to receiving a communication from a second user:
 - determining whether the display name of the second user is equivalent to the display name of a user in the contact data store; and
- when the display name of the second user is equivalent to the display name of a ~~stored contact user~~ in the contact data store, and the identity of the second user is different than the identity of the user in the contact data store with the matching display name, generating a warning on a display associated with

the computing device, wherein generating the warning comprises generating a warning about a potentially masquerading user having a display name equivalent to the display name of the user in the contact data store with the matching display name, the potentially masquerading user selected from a set of users having display names equivalent to the display name of the user in the contact data store with the matching display name, the set including the user in the contact data store with the matching display name, and the potentially masquerading user being selected based on relative authorization levels of the users in the set, wherein:

the warning comprises a name conflict indicator displayed in a first graphical user interface to the computing device indicating a conflict with a conflicted display name, the conflicted display name being the display name common to the second user and the user in the contact data store with the matching display name; and

the method further comprises:

in response to user input received through the first graphical user interface, the user input being associated with the name conflict indicator, displaying on the computing device a plurality of equivalent display names that are equivalent to the conflicted display name;

receiving user input from a user of the computing device specifying an alternative display name for a selected display name, the alternative display name being selected by the user from the plurality of equivalent display names displayed on the computing device, the alternative display name being associated with a selected identity and being different than the conflicted display name; and

identifying on a second graphical user interface of the computing device the selected identity with the alternative display name, the second graphical user interface providing a function related to controlling communication within the peer-to-peer collaboration system, the communication being between the computing device and a second device associated with the selected identity.

44. (Previously Presented) The method of claim 43, further comprising, for each of a plurality of instances of the display name of the second user appearing on a display screen of the computing device, displaying the warning in conjunction with the display name.

45. (Previously Presented) The method of claim 44, wherein at least one of the plurality of instances comprises a listing of contacts in a graphical user interface adapted to receive user input selecting a contact with which to communicate.

46. (Previously Presented) The method of claim 43, wherein generating the warning in conjunction with the display name comprises displaying an icon adjacent an instance of the display name.

47. (Previously Presented) The method of claim 43, further comprising:

upon receiving a communication from a new user for which there is no entry in the contact data store, making an entry for the new user in the contact data store, the making an entry comprising displaying a graphical user interface presenting information about the new user and containing an input area adapted to receive input from a user of the computing device authenticating the new user.

48. (Previously Presented) The method of claim 47, wherein:

when the input from the user of the computing device authenticating the new user is received, storing in the entry for the new user an indication that the new user is authenticated;
and

when the input from the user of the computing device authenticating the new user is not received, storing in the entry for the new user an indication that the new user is unauthenticated.

49. (canceled)

50. (Cancelled)

51. (Previously presented) A method of operating a computing device providing an endpoint in a peer-to-peer collaboration system in which each user has an identity and a display name, the method comprising:

- receiving an input setting a security policy from a user of the computing device and/or a system administrator;

- in response to an event that triggers a function that includes display of a display name of a first user:

- determining an authentication level of the first user, the authentication level comprising an authentication level being selected from a set comprising a certified level, an authenticated level, and an unauthenticated level, the certified level being higher than the authenticated level and the authenticated level being higher than the unauthenticated level;

- selectively responding to the event based on the authentication level and the security policy, the security policy having at least an allow option, a restrict option and a warn option, and the selectively responding comprising:

- when the security policy option is determined to be allow, presenting on a graphical user interface the display name of the first user in conjunction with performance of the function in response to the event;

- when the security policy option is determined to be warn and the authentication level is less than or equal to a threshold level, presenting on the graphical user interface the display name of the first user in conjunction with performance of the function, the presenting including presenting a warning on the authentication level of the first user; and

- when the security policy option is set to restrict and the authentication level is less than or equal to the threshold level, omitting performance of the function.

52. (Previously Presented) The method of claim 51, wherein the threshold level is determined dynamically based on an authentication level of at least one other user having a display name equivalent to the display name of the first user.

53. (Previously Presented) The method of claim 51, wherein the selectively responding comprises processing the event based on the authentication level and a security policy and the nature of the response to the event.

54. (Previously Presented) The method of claim 51, further comprising:

upon receiving a communication from a new user for which there is no entry in a contact data store, making an entry for the new user in the contact store, the making an entry comprising displaying a graphical user interface presenting information about the new user and containing an input area through which a user of the computing device can authenticate the new user.

55. (Previously Presented) The method of claim 51, wherein the event comprises receiving a communication from the first user.

56. (Previously Presented) The method of claim 51, wherein the event comprises receiving user input including a command to initiate communication with a user.

57. (Canceled)

58. (Currently amended) A computer storage medium comprising computer-executable instructions that, when executed on a computing device providing an endpoint in a peer-to-peer collaboration system in which each user has an identity and a display name, perform a method comprising:

receiving an input setting a security policy from a user of the computing device and/or a system administrator;

in response to an event that triggers a function that includes display of a display name of a first user:

determining an authentication level of the first user, the authentication level comprising an authentication level being selected from a set comprising a certified level, an authenticated level, and an unauthenticated level, the certified level being higher than the authenticated level and the authenticated level being higher than the unauthenticated level;

selectively responding to the event based on the authentication level and [[a]] the security policy, the security policy having at least an allow option, a restrict option and a warn option, and the selectively responding comprising:

when the security policy option is determined to be allow, presenting on a graphical user interface the display name of the first user in conjunction with performance of [[a]] the function performed in response to the event;

when the security policy option is determined to be warn and the authentication level is less than or equal to a threshold level, presenting on the graphical user interface the display name of the first user in conjunction with performance of the function, the presenting including presenting a warning on the authentication level of the first user, wherein when the first user is not determined to be certified, the method comprises:

displaying a graphical user interface presenting information about the first user and containing an input area adapted to receive input from a user of the computing device authenticating the first user;

when input is received from the user of the computing device authenticating the first user, determining that the first user has an authentication level of authenticated; and

when input is not received from the user of the computing device authenticating the first user, determining that the first user has an authentication level of unauthenticated; and

when the security policy option is set to restrict and the authentication level is less than or equal to the threshold level, omitting performance of the function.

59. (Currently amended) A computer storage medium comprising computer-executable instructions that, when executed on a computing device providing an endpoint in a peer-to-peer collaboration system in which each user has an identity and a display name, perform a method comprising:

in response to an event adapted to trigger a function associated with a first user different than a user of the computing device:

determining an authentication level of the first user, the authentication level comprising an authentication level being selected from a set comprising a certified level, an authenticated level, and an unauthenticated level, the certified level being higher than the authenticated level and the authenticated level being higher than the unauthenticated level;

selectively responding to the event based on the authentication level and a security policy, the security policy having at least an allow option, a restrict option and a warn option, and the selectively responding comprising:

when the security policy option is set to restrict and the authentication level is less than or equal to [[the]] a threshold level, blocking performance of the function; and

when the security policy option is determined to be warn and the authentication level is less than or equal to the threshold level, presenting on a graphical user interface the display name of the first user in conjunction with performance of the function in response to the event, the presenting including presenting a warning on the authentication level of the first user,

wherein:

the authentication level comprises an authentication level selected from a set comprising a certified level, an authenticated level, and an unauthenticated level, the certified

level being higher than the authenticated level and the authenticated level being higher than the unauthenticated level; and

the method further comprises:

when the first user is not determined to be certified;

displaying a graphical user interface presenting information about the first user and containing an input area adapted to receive input from a user of the computing device authenticating the first user;

when input is received from the user of the computing device authenticating the first user, determining that the first user has an authentication level of authenticated; and

when input is not received from the user of the computing device authenticating the first user, determining that the first user has an authentication level of unauthenticated.

60. (Cancelled)

61. (Currently amended) The computer storage medium of claim [[60]] 59, wherein determining the authentication level of the first user comprises accessing a contact data store in memory associated with the computing device.

62. (Previously Presented) The computer storage medium of claim 61, wherein the method further comprises, prior to the event, in response to communicating with the first user, recording the first user as a contact in the contact data store, the recording comprising storing at least an identity, display name and authentication level of the first user.

63. (Currently amended) The computer storage medium of claim 62, wherein ~~the method further comprises, determining the authentication level of the first user~~[[.]] ~~the determining comprising~~ further comprises:

displaying a graphical user interface presenting information about the first user and containing an input area adapted to receive input from the user of the computing device authenticating the first user; and

when input is received from the user of the computing device authenticating the first user, determining that the first user has an ~~authenticated~~ authentication level of authenticated.

64. (Currently amended) The computer storage medium of claim 62, ~~wherein the method further comprises, determining the authentication level of the first user[[,]] the determining comprising~~ further comprises:

receiving information on authentication level of users of the peer-to-peer collaboration system from a network administrator; and

when the received information comprises an indication that the first user is certified, determining that the authentication level of the first user is certified.

65. (Canceled)